White Paper

The Federal Privacy Act of 1974 and HIPAA Privacy Rule of 1996: A Comparison

September 2007

Introduction

While health care providers have a long tradition of safeguarding private health information, protection of patient rights has recently been at the forefront of discussion. The old system of storing private patient information in locked filing cabinets is no longer practical or feasible—modern technology now allows for the rapid transmission of medical information electronically. However, along with this ease of sharing come new concerns regarding the confidentiality and protection of patient information. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule of 1996 provides clear standards for protection of personal health information or Protected Health Information (PHI). Prior to the Privacy Rule, PHI could be distributed without notice or authorization by the patient for reasons other than the patient's medical treatment and/or health care payment. While improving the efficiency of the healthcare delivery system, the act protects the privacy of PHI by simplifying the processes involved in transmitting data by standardizing electronic data interchange. This act sought to close a gap in the 1974 Privacy Act, which provided some safeguards to the collection and use of personal information by the federal government and its entities.

The Privacy Act of 1974, Public Law 93-579

The Privacy Act of 1974 provides individuals the right of access to information concerning themselves that is maintained by any federal agency in the Executive Branch. The Act also established controls over what personal information the federal government collects and how it uses or discloses that information. The Act arose out of concerns about how the creation and use of computerized databases might impact individuals' privacy rights. It safeguards privacy with the use of four personal data rights:

- Government agencies must show an individual any records kept on him or her;
- Agencies must follow certain principles, called "fair information practices," regarding personal data.
- Agencies are restricted in how they can share individual data with other people and agencies;
- Individuals may sue the government for violating the Act's provisions.

Health Insurance Portability and Accountability Act of 1996

The HIPAA Privacy Rule *(45 CFR Parts 160 and 164)*

HIPAA improves the efficiency and effectiveness of the health care industry in three primary ways; 1) by administrative simplifications provisions that develop single and universal claims and payment transaction codes, 2) by protecting the privacy and security of PHI, and 3) by providing provisions for the enforcement of its rules. The scope of HIPAA encompasses the following entities: health care plans, health care clearinghouses, and all health care providers who conduct certain health care transactions electronically.

The Privacy Rule is the foundation for federal protection for the privacy of PHI. PHI includes individually identifiable health information related to the past, present or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Even the fact that an individual received medical care is protected information under the regulation.

Privacy Rights

Together, the 1996 HIPPA Privacy Rule and the 1974 Privacy Act allow patients more rights and control over personal and medical information. In combination the acts do the following:

- Set boundaries on the use and release of personal data;
- Generally limit release of information to the minimum reasonably needed for the purpose of the disclosure.
- Establish safeguard standards for protecting the privacy of personal data.
    - Enable individuals to learn how their data may be used and about certain disclosures of their data that have been made
    - Empower individuals to control certain uses and disclosures of their personal data.
- Generally give individuals the right to examine and obtain a copy of their own personal data and request corrections.
- Hold violators accountable, with civil and criminal penalties that can be imposed if they violate individuals' rights.

Oversight

The Privacy Act empowers the Director of the Office of Management and Budget to develop regulations and guidelines on how agencies should implement the Act.

HIPAA empowers Health and Human Services (HHS) Office for Civil Rights to enforce the Privacy Rule by promoting voluntary compliance and using civil monetary penalties.

Penalties for Violations of Privacy

Both acts impose penalties on violators. The HIPAA Privacy Rule is the stricter of the two, imposing both civil and criminal penalties for violations of privacy. Penalties are generally assessed when organizations or individuals act with willful neglect or intent to cause harm. Civil penalties are specified at $100 per violation, not to exceed $25,000 per person per year for identical violations. Criminal penalties for wrongful disclosure of PHI can go up to $250,000 and/or 10 years imprisonment if the offense is committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm.

The 1974 Privacy Act gives an individual the right to sue the federal government if it violates the statue. In addition:

- Any officer or employer of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information, and conveys that information to any person or agency not entitled to receive it shall be guilty of a misdemeanor and fined not more than $5,000.
- Any officer or employee of an agency who willfully maintains a system of records for personal use shall be guilty of a misdemeanor and fined not more that $5000.

Any person who knowingly and willfully requests or obtains and record concerning an individual from an agency under false pretense shall be guilty of a misdemeanor and fined not more than $5000.

Discussion

The purpose of both acts was to strengthen the rights of the public in regards to the collection and use private information. Both work together to achieve the goal of protecting the privacy of personal information. Though HIPAA focuses mainly on medical information, the HIPAA Privacy Rule provision strengthens the intent of the Privacy Right Act of 1974 in that it requires all Federal agencies and/or Federal contractors that maintain personal records of individuals to adhere to the Privacy Rule's requirements and comply with the Privacy Act.

Comments

The Acts differ in that the 1974 Act covers overall personal data collection and use by the federal government, not private entities. HIPAA seeks to close this gap by targeting an industry that has more information on the public than the government—the medical field. HIPAA is more specific because it only targets medical information—but it is far reaching because it closes all of this personal data off to others, including the government, if they cannot show a compelling interest for having access to this data.